Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2015 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2015

Social Networking Behaviors: Role of personality, perceived risk, and social influences

Tejaswini Herath
Brock University, Canada, teju.herath@brocku.ca

John D'Arcy
University of Delaware, USA, jdarcy@udel.edu

R64. Social Networking Behaviors: Role of personality, perceived risk, and social influences

Tejaswini Herath,
Brock University, Canada,
teju.herath@brocku.ca

John D'Arcy,
University of Delaware, USA,
jdarcy@udel.edu

Abstract

With the growth in use of social media, various security and privacy concerns are burgeoning. Motivated by the phenomenon of OSN use and the potentially risky behaviors it involves, the present study has two main objectives: (1) to understand the effect of individuals' perceived risk on OSN use and risky OSN behaviors; and (2) to understand the role of social influence on OSN use and risky OSN behaviors. In this work in progress a theoretical model is developed for an empirical examination.

1. Introduction

Social media use has grown dramatically across all age groups in recent years. Online social networks (OSN) provide a platform that allows people to communicate more efficiently with their friends, family, and colleagues. The use of social media, however, is not without problems. Newspapers have reported many incidents where sharing information on OSNs such as Facebook, Twitter, MySpace, or YouTube has cost individuals their job, money, marriage, or even freedom. These threats are also real in the organizational context. The use of OSN in the workplace is widespread, and the inadvertent disclosure of proprietary information is a major concern [Kaplan and Haenlein, 2010], as are other security issues such as the spread of malware [Ponemon Institute, 2011]. Most respondents in a recent Ponemon security survey (2011) agreed that the use of social media in the workplace is important to achieving business objectives; however, respondents also felt that OSN usage put their organizations at risk and that their organizations lacked the necessary security controls and enforceable policies to address the risk.

Motivated by the phenomenon of OSN use and the potentially risky behaviors it involves, the present study has two main objectives: (1) to understand the effect of individuals' perceived risk on OSN use and risky OSN behaviors; and (2) to understand the role of social influence on OSN use and risky OSN behaviors. Given the "social" nature of OSN use, we apply the theory of differential association from the literature in criminology and delinquency to examine the aforementioned research questions. Differential association theory considers an individual's social reference group as having a strong influence on delinquent/criminal behaviors. We integrate this perspective with longstanding research on individual risk perception and personality to assess the relative influences of the social vs. individual drivers of OSN use. Our

aim is to advance the current understanding of the factors that influence both regular and risky OSN usage behaviors and, more broadly, to contribute to the behavioral IS security research that considers insecure user behaviors.

The paper proceeds as follows. In the next section, we present a theoretical background and proposed hypotheses; then we present the methodology adopted in this study.

2. OSN Use

OSN is a platform that allows people to communicate efficiently with their friends, family, and colleagues. A number of articles report a complex set of social factors as the reasons for OSN use [Ellison et al., 2007, Joinson, 2008, Lampe et al., 2008, Muscanell and Guadagno, 2011, Skeels and Grudin, 2009]. These factors include various types of messages, photos, and other media sharing interactions (e.g., status updates) used to find, meet, and keep in touch with the members of a user's network [Joinson, 2008]. Recent surveys also list many negative outcomes associated with OSN usage. For example, the following negative outcomes have occurred to frequent OSN users [Madden, 2010]: ending of a friendship due to a OSN, a OSN experience that resulted in a face-to-face argument or confrontation, teens facing problems with their parents due to a OSN, a physical fight with someone based on an experience they had with a OSN, and getting in trouble at work or at school because of a OSN exchange. From an organizational perspective, industry surveys have identified employees downloading apps or widgets from OSNs and posting uncensored content and uncensored blog entries as threats to information security. Further to this point, malware infections are increasing as a result of social media use, and organizations are facing bandwidth issues [Ponemon Institute, 2011]. Organizations are also concerned with productivity losses due to the time employees spend on OSNs during work hours [Kaplan and Haenlein, 2010]. Clearly, while it provides a platform for employee engagement in work-related matters, OSN usage can have drawbacks that include threats to an organization's information security. In this paper, in addition to regular OSN use, we consider two risky OSN behaviors that have direct relevance to information security: (1) forwarding messages that possibly contain malware, and (2) sharing sensitive information via OSNs (i.e., data leakage).

3.0 Hypotheses Development

3.1 Perceived Risk

Decision making is influenced by risk taking propensity and risk perception [Sitkin and Pablo, 1992]. Recently there has been a significant consideration of risks in various computing activities and their impact on user behavior. Research shows that these risks affect user behavior in a variety of ways. Users can opt out of behaviors considered to be risky [Chen et al., 2011], including intention to transact on-line [Luo et al., 2010, Pavlou, 2003]. Users can also put in additional effort in evaluating a risk decision [Wang et al., 2009] or use security technologies that aid in reducing risk [Herath et al., 2014, Wang et al., 2009]. A review of the related IS security literature also suggests that individuals' security practices may be understood as a coping mechanism in the face of perceived cyber threats [Herath and Rao, 2009, Johnston and Warkentin, 2010, Liang and Xue, 2010, Liang and Xue, 2009, Workman et al., 2008]). Rooted in protection motivation theory (PMT) and coping theories, this literature proposes that technology

users faced with threats in computing environments first appraise the existence and degree of the threat and then assess what they can do to avoid it. Existing empirical studies suggest that when people perceive a threat as severe and likely, they undertake measures that they think are effective in preventing that threat, such as taking protective action or abstaining from the risky behavior [Chen et al., 2011, Choi et al., 2008, Herath et al., 2014, Herath and Rao, 2009, Wang et al., 2009]. In the context of OSN use, if the user feels that in general the OSN environment poses a threat, s/he is more likely to avoid OSN use, while if the user perceives the risk to be low, s/he is likely to continue the frequent OSN usage. In terms of the risky OSN behaviors in our study, individuals who perceive higher levels of risks in information sharing activities are likely to abstain from carrying out such acts compared to those who do not perceive such acts as risky. Messages and links sent via OSNs may at times pose considerable risks as they are frequently employed by malicious parties as attack vectors to spread malicious code such as virus, worms, and other malware. We expect that individuals who believe that these types of messages are harmful will be reluctant to forward these messages.

H1: Perceived OSN Threats→ (-) OSN Regular Use

H2: Perceived risks of Insecure OSN Behavior → (-) Insecure OSN Behavior Likelihood

3.2 Social Learning - Differential Association

By its very nature, OSN use has a strong social component. In this regard, we consider social influences as important drivers of regular and risky OSN use. Social influences have a long history in the IS literature. A norm, or social norm, can be a reason to act, believe, or feel. Social influence, which is the extent to which one member's social network influences behavior, is exerted through messages about expectations which help form perceptions of the value of an activity as well as the observed behavior of others [Venkatesh and Brown, 2001].

Sutherland's theory of differential association [Sutherland, 1947] proposes that like any other social behavior, delinquent behavior is learned from others. This theory was later enhanced as a social learning theory. Social learning theory [Akers, 1977] explains that delinquent behavior is a result of social and cultural factors that motivate and control behavior [Akers and Jensen, 2010]. The theory encompasses four major explanatory concepts or dimensions – differential association, definitions (and other discriminative stimuli), differential reinforcement, and imitation. *Differential association* refers to direct association and interaction with others who engage in certain kinds of behavior or express norms, values, and attitudes supportive of this behavior. People, in interaction with significant groups, learn evaluative *definitions* of a behavior in terms of whether the behavior is good or bad. Individuals may also engage in behavior by *imitation* after observing similar behavior by others. *Differential reinforcement,* which refers to the balance of anticipated or actual rewards and punishments that follow or are the consequences of behavior, will influence individuals' likelihood of committing a crime at any given time [Akers and Jensen, 2010]. This notion is also echoed in the literature on deterrence theory.

Social media use is highly likely to be affected by the social influence exerted by significant others. Social influence, considered in this study in form of subjective norms, is a belief as to whether or not significant others want an individual to engage in OSN use. The view that individuals are more likely to comply with significant others' expectations when those others have the ability to reward the desired behavior or punish non-compliant behavior is consistent with findings in the technology acceptance literature. While the IT use literature has used a variety of labels for this construct, each of these constructs contains the notion that the

individual's behavior is influenced by what the significant others expect her/him to do [Venkatesh et al., 2003]. If an individual believes that her/his peers, family, parents, etc., do not expect her/him to use or extensively use an OSN, the likely result is reduced OSN usage by that individual. However, if this group of significant others approves or encourages the individual's OSN usage, s/he is more likely to use the OSN.

H 3: Social influence related to OSN use → (+) OSN Regular Use

Similar to the social influence considered in the section above, prior literature in delinquency informs us that social influence can impact not only positive behaviors but also negative behaviors [Akers and Jensen, 2010]. Associations with those who are deviant provide individuals with "attitudes favorable" to the delinquent behavior and have been found to be very powerful influences towards such behavior [Akers and Jensen, 2010]. These delinquent groups provide social environments in which an individual creates definitions of behavior and is exposed to imitation models and various social reinforcements for deviant behavior. Rogers and Buffalo [Rogers and Buffalo, 1974] found that delinquents conform to the norms of their community. Hindlelang (1974) examined the aspect of peer commitment to delinquent acts and found that when individuals perceive that peers approve of delinquent acts, they are "propelled or pulled" into committing deviant acts in order to fulfill group membership or peer expectations.

If an individual believes that her/his referent group would disapprove of a particular behavior such as posting sensitive information on OSNs, s/he is more likely to refrain from this behavior. On the other hand, if an individual believes that this group of significant others would approve of this behavior, then s/he is more likely to undertake the deviant behavior.

H4 → Peer influence related to insecure OSN behavior → (+) insecure OSN behavior Likelihood

In differentiated association, groups also provide an opportunity to imitate behavior [Akers and Jensen, 2010]. Theory also suggests that imitation, although most important in the initial stages, continues to have some effect in maintaining behavior. A similar notion is considered under the umbrella of descriptive norms. Descriptive norms, referred to as the extent to which one believes others are performing a behavior, increases a propensity an individual may have to indirectly reciprocate the believed behavior of others [Sheeran and Orbell, 1999]. Here the individual's behavior is motivated by observing what the typical or normal thing to do is. It is what most people do and "if everyone is doing it, it must be sensible thing to do" [Cialdini et al., 1990]. People often do (or believe in) certain actions or non-actions because many other people do (or believe) the same. The technology acceptance literature has found support for the role of peer behaviors as a motivational source for performing a behavior [Thompson et al., 1994, Venkatesh et al., 2003].

This influence has also been found to be an influential source for negative behaviors. In a paper titled "Monkey see monkey do…," Robinson and O'Leary-Kelly [Robinson and O'Leary-Kelly, 1998] found that antisocial behaviors at work are shaped by the antisocial behaviors of coworkers. Similarly, much evidence in the digital piracy literature shows that if individuals believe others are pirating, they do not fear sanctions. Turning to our insecure OSN behaviors, if an individual believes that others are doing the same, s/he is likely to cognitively diminish or reduce the level and possibility of sanctions imposed and thus will lean toward continuing the act. Conversely, if an individual thinks that nobody else is carrying out such acts, s/he is more likely to refrain from the act.

H5→ Peer behavior Likelihood related to insecure OSN behavior → (+) insecure OSN behavior likelihood

3.3 Personality: Need to Belong

All people have a pervasive need to be socially accepted and to belong to social groups [Baumeister and Leary, 1995]. Personality characteristics have been posited as having a strong influence on OSN use [Correa et al., 2010], and this personality characteristic known as need to belong, which captures social needs and motivations, is an important consideration in the context of social media usage and social inclusion. The forming of social bonds is important to all people [Hornsey and Jetten, 2004]. Although the need to belong is almost universal and almost all normal individuals desire to be accepted and to belong to social groups, the strength and intensity of this need varies among people [Baumeister and Leary, 1995, Leary et al., 2013]. Because of the strength of the need to belong varies among people, its effect emerges in varying levels of attitudes and willingness by different people to join and participate in user-generated content sites. In other words, there is a greater chance that people will join and participate in OSNs if they rate high on the need to belong scale. OSN users are doing more than just sharing information and connecting with their friends, they are creating a virtual community and forming real bonds with others who are in their network. By discontinuing his or her acts of OSN usage, a OSN user is not only giving up the ability to share emotions and experiences with other community members, but also the ability to fully take part in this subculture and experience the related joys. Social bonds keep individuals invested in a particular subculture [Bainbridge, 1990]. The OSN user has much to lose - the potential loss of a community of like-minded individuals. Hence, we believe:

H6 → Need to belong → (+) OSN regular use

H7→ Need to belong → (+) insecure OSN behavior likelihood

Based on the preceding arguments, we propose the research model presented in Figure 1.

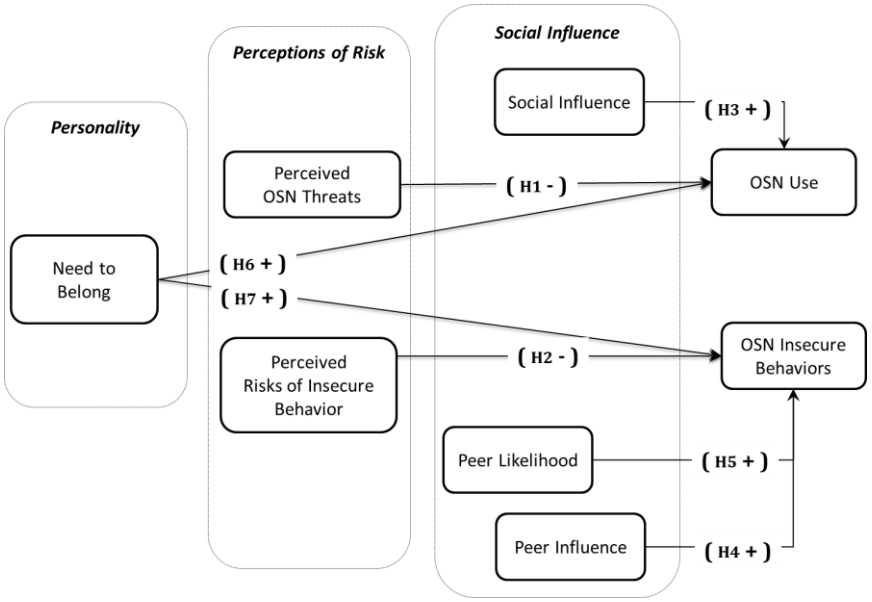

Figure 1:

4.0 Methodology

To test the proposed research model, data will be collected using a survey with a cross-sectional design. Self-administered surveys that provide anonymity are a well suited method of inquiry, especially regarding delinquent behaviors, since they can offer privacy to the respondent and are recommended where possibly sensitive answers are sought. Since our intent is to understand OSN practices from an organizational context and we want to capture both students and employees in our sample, we are using a professional market research firm to randomly select and invite participants to take our survey. The results will be ready for presentation at the workshop in May.

References

Akers, R. L. (1977) "Deviant behavior: A social learning approach."

Akers, R. L. and G. F. Jensen (2010) "Social Learning Theory: Process and Structure in Criminal and Deviant Behavior," *The SAGE Handbook of Criminological Theory* pp. 56.

Bainbridge, W. S. (1990) "Explaining the church member rate," *Social Forces* (68) 4, pp. 1287-1296.

Baumeister, R. F. and M. R. Leary (1995) "The need to belong: desire for interpersonal attachments as a fundamental human motivation," *Psychological bulletin* (117) 3, pp. 497.

Chen, R., J. Wang, T. Herath, and H. R. Rao (2011) "An investigation of email processing from a risky decision making perspective," *Decision support systems* (52) 1, pp. 73-81.

Choi, N., D. Kim, J. Goo, and A. Whitmore (2008) "Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action," *Information Management & Computer Security* (16) 5, pp. 484-501.

Cialdini, R. B., R. R. Reno, and C. A. Kallgren (1990) "A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places," *Journal of Personality and Social Psychology* (58) 6, pp. 1015-1026.

Correa, T., A. W. Hinsley, and H. G. De Zuniga (2010) "Who interacts on the Web?: The intersection of users' personality and social media use," *Computers in Human Behavior* (26) 2, pp. 247-253.

Ellison, N. B., C. Steinfield, and C. Lampe (2007) "The benefits of Facebook "friends:" Social capital and college students' use of online social network sites," *Journal of Computer-Mediated Communication* (12) 4, pp. 1143-1168.

Herath, T., R. Chen, J. Wang, K. Banjara et al. (2014) "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service," *Information Systems Journal* (24) 1, pp. 61-84.

Herath, T. and H. R. Rao (2009) "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* (18) 2, pp. 106-125.

Hornsey, M. J. and J. Jetten (2004) "The individual within the group: Balancing the need to belong with the need to be different," *Personality and Social Psychology Review* (8) 3, pp. 248-264.

Johnston, A. C. and M. Warkentin (2010) "Fear appeals and information security behaviors: An empirical study," *MIS quarterly* (34) 1, pp. 1-20.

Joinson, A. N. (2008) Looking at, looking up or keeping up with people?: motives and use of facebook. *Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems, 2008*, pp. 1027-1036.

Kaplan, A. M. and M. Haenlein (2010) "Users of the world, unite! The challenges and opportunities of Social Media," *Business horizons* (53) 1, pp. 59-68.

Lampe, C., N. B. Ellison, and C. Steinfield. (2008) Changes in use and perception of Facebook. *Proceedings of the 2008 ACM conference on Computer supported cooperative work, 2008*, pp. 721-730.

Leary, M. R., K. M. Kelly, C. A. Cottrell, and L. S. Schreindorfer (2013) "Construct validity of the need to belong scale: Mapping the nomological network," *Journal of personality assessment* (95) 6, pp. 610-624.

Liang, H. and Y. Xue (2010) "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information System* (11) 7, pp. 394-413.

Liang, H. G. and Y. J. Xue (2009) "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33) 1, pp. 71-90.

Luo, X., H. Li, J. Zhang, and J. Shim (2010) "Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services," *Decision support systems* (49) 2, pp. 222-234.

Madden, M. (2010) "Older Adults and Social Media: Social networking use among those ages 50 and older nearly doubled over the past year," http://pewinternet.org/Reports/2010/Older-Adults-and-Social-Media.aspx (October 21, 2013).

Muscanell, N. L. and R. E. Guadagno (2011) "Make new friends or keep the old: Gender and personality differences in social networking use," *Computers in Human Behavior*.

Pavlou, P. A. (2003) "Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model," *International journal of electronic commerce* (7) 3, pp. 101-134.

Ponemon Institute (2011) "Ponemon Institute Research Report: Global Survey on Social Media Risks (Survey of IT & IT Security Practitioners)," www.websense.com/content/ponemon-institute-research-report-2011.aspx (October 21, 2013).

Robinson, S. L. and A. M. O'Leary-Kelly (1998) "Monkey see, monkey do: The influence of work groups on the antisocial behavior of employees," *Academy of Management Journal* (41) 6, pp. 658-672.

Rogers, J. W. and M. D. Buffalo (1974) "Fighting back: Nine modes of adaptation to a deviant label," *Social Problems* pp. 101-118.

Sheeran, P. and S. Orbell (1999) "Augmenting the Theory pf Planned Behvaior: Roles for Anticipated Regret and Descriptive Norms," *Journal of Applied Social Psychology* (29) 10, pp. 2107-2142.

Sitkin, S. B. and A. L. Pablo (1992) "Reconceptualizing the Determinants of Risk Behavior," *The Academy of Management Review* (17) 1, pp. 9-38.

Skeels, M. M. and J. Grudin. (2009) When social networks cross boundaries: a case study of workplace use of facebook and linkedin. *Proceedings of the ACM 2009 international conference on Supporting group work, 2009*, pp. 95-104.

Sutherland, E. H. (1947) "Differential association."
Thompson, R. L., C. A. Higgins, and J. M. Howell (1994) "Influence of Experience on Personal Computer Utilization," *Journal of Management Information Systems* (11) 1, pp. 167-187.
Venkatesh, V. and S. Brown (2001) "A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges," *MIS Quarterly* (25) 1, pp. 71-102.
Venkatesh, V., M. G. Morris, G. B. Davis, and F. D. Davis (2003) "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27) 3, pp. 425-478.
Wang, J., R. Chen, T. Herath, and H. R. Rao (2009) "Visual e-mail authentication and identification services: An investigation of the effects on e-mail use," *Decision support systems* (48) 1, pp. 92-102.
Workman, M., W. H. Bommer, and D. Straub (2008) "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24) 6, pp. 2799-2816.